Xerox Security Bulletin XRX11-003

FreeFlow Print Server
Oracle July 2011 CPU OS and Security Patch Cluster (includes Java 6 Update 26 Software)
v1.0
08/19/11

Background

Oracle delivers quarterly Critical Patch Updates (CPU) to address US-CERT-announced Security vulnerabilities and deliver reliability improvements to the Solaris Operating System. Oracle no longer provides these patches to the general public, but Xerox is authorized to deliver them to Customers with active FreeFlow Print Server (FFPS) Support contracts (FSMA). Xerox customizes the patch deliveries as appropriate to each FFPS Product family, and tests the CPU patches on each supported SPAR Release prior to delivery. Customers who may have an Oracle Support Contract for their non-FFPS Solaris Servers should not install patches that have not been customized by Xerox. Otherwise the FFPS software could be damaged and result in downtime and a lengthy re-installation service call.

This bulletin announces the availability of the following:

1. Oracle July 2011 CPU OS and Security Patch Cluster
   - ✓ This supersedes the Oracle April 2011 CPU Cluster
2. Java 6 Update 26 Software
   - ✓ This supersedes Java 6 Update 24 Software

The Security vulnerabilities that are remediated with this Oracle Security patch delivery are as follows:

CVE-2011-0579	**CVE-2011-0618**	**CVE-2011-0619**	**CVE-2011-0620**	**CVE-2011-0621**
CVE-2011-0622	**CVE-2011-0623**	**CVE-2011-0624**	**CVE-2011-0625**	**CVE-2011-0626**
CVE-2011-0627	**CVE-2011-0628**	**CVE-2011-1910**	**CVE-2011-2245**	**CVE-2011-2249**
CVE-2011-2258	**CVE-2011-2259**	**CVE-2011-2285**	**CVE-2011-2287**	**CVE-2011-2289**
CVE-2011-2290	**CVE-2011-2291**	**CVE-2011-2294**	**CVE-2011-2295**	**CVE-2011-2298**

Note: Xerox recommends that customers evaluate their security needs periodically and if they need security patches to address the above CVE issues, schedule an activity with their Xerox Service team to install the Critical Patch Updates.

Applicability

These Security updates are intended for Xerox printer products running one of the FFPS SPAR software releases below:

1. 73.A3.31
2. 73.B0.73

This Security patch software has only been tested on these software releases and should not be installed on any other FFPS software release. The Xerox CSE/Analyst is provided a tool that enables them to confirm the currently installed FFPS software release, Oracle Security Patch Cluster, and Java Software version. Below is an example of the standard output from this script:

FFPS Release Version: 7.0_SP-3 (73.A3.31.86)
Oracle Cluster: January 2011
Java Version: Java 6 Update 22

Patch Install Methods

The install of these Security patches must be performed by the Xerox Customer Service Engineer (CSE) or Analyst. The customer process to obtain this Security update is to contact the Xerox hotline to initiate a Log number to track the activity.

Xerox strives to deliver these critical Security patches in a timely manner. They are available from the Xerox Support organization, and can be delivered electronically over the Internet to FFPS via a GUI tool called the FFPS Update Manager. The other method of delivery is by ordering DVD/USB media. The methods used by the CSE/Analyst to install the Security patches are as follows:

Update Manager GUI

Once the Security patches are ready for customer delivery they are made available from the Xerox Edge and Download servers. The CSE/Analyst uses the Update Manager GUI on the FFPS system to download and install the Security patches over the Internet. This requires that the FFPS system be configured with the customer proxy information to gain Xerox server access of the Security patches. The connection is initiated by the FFPS system and the Xerox server does not have access to the customer network. The Xerox server and FFPS system both authenticate each other before a data transfer can be successfully established between the two end points.

DVD/USB Media

Once the Security patches are ready for customer delivery they are made available on DVD/USB media. The CSE/Analyst will need access to either the DVD or USB devices on the FFPS platform to install these Security patches.

Disclaimer